United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001)

32-41 minutes

U.S. District Court for the District of New Jersey - 180 F. Supp. 2d 572 (D.N.J. 2001)
December 26, 2001

180 F. Supp. 2d 572 (2001)
UNITED STATES,
v.
Nicodemo S. SCARFO, et al.
Criminal Action No. 00-404 (NHP).

United States District Court, D. New Jersey.

December 26, 2001.

***573 *574** Vincent C. Scoca, Bloomfield, NJ, Norris E. Gelman, Philadelphia, PA, for Nicodemo S. Scarfo.

Richard M. Roberts, West Orange, NJ, for Frank Paolercio.

Ronald D. Wigler, Assistant United States Attorney, Robert J. Cleary, United States Attorney, Newark, NJ, for United States.

THE ORIGINAL OF THIS LETTER OPINION AND ORDER IS ON FILE WITH THE CLERK OF THE COURT

POLITAN, District Judge.

Dear Counsel:

This matter comes before the Court on Defendant Nicodemo S. Scarfo's ("Scarfo") pretrial motion for discovery and suppression of evidence. The Court heard oral argument on July 30, 2001 and again on September 7, 2001. Co-defendant Frank Paolercio ("Paolercio") joined in the motion. The government thereafter moved to invoke the Classified Information Procedures Act. For the following reasons, the Defendants' motion for discovery is granted in part and denied in part, and the motion to suppress evidence is denied.

BACKGROUND

This case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity. It appears that no district court in the country has addressed a similar issue. Of course, the matter takes on added importance in light of recent events and potential national security implications.

The Court shall briefly recite the facts and procedural history of the case. Acting pursuant to federal search warrants, the F.B.I. on January 15, 1999, entered Scarfo and Paolercio's business office, Merchant Services of Essex County, to search for evidence of an illegal gambling and loansharking operation. During their search of Merchant Services, the F.B.I. came across a personal computer and attempted to access its various files. They were unable to gain entry to an encrypted file named "Factors."

Suspecting the "Factors" file contained evidence of an illegal gambling and loansharking operation, the F.B.I. returned to the location and, pursuant to two search warrants, installed what is known as a "Key Logger System" ("KLS") on the computer and/or computer keyboard in order to decipher the passphrase to the encrypted file, thereby gaining entry to the file. The KLS records the keystrokes an individual enters on a personal computer's keyboard. The government utilized the KLS in order to "catch" Scarfo's passphrases to the encrypted file while he was entering them onto his keyboard. Scarfo's personal computer features a modem for communication over telephone lines and he possesses an America Online account. The F.B.I. obtained the passphrase to the "Factors" file and retrieved what is alleged to be incriminating evidence.

On June 21, 2000, a federal grand jury returned a three-count indictment against the Defendants charging them with gambling and loansharking. The Defendant Scarfo then filed his motion for discovery and to suppress the evidence recovered from his computer. After oral argument was heard on July 30, 2001, the Court ordered additional briefing by the parties. ***575** In an August 7, 2001, Letter Opinion and Order, this Court expressed serious concerns over whether the government violated the wiretap statute in utilizing the KLS on Scarfo's computer. Specifically, the Court expressed concern over whether the KLS may have operated during periods when Scarfo (or any other user of his personal computer) was communicating via modem over telephone lines, thereby unlawfully intercepting wire communications without having applied for a wiretap pursuant to Title III, 18 U.S.C. § 2510.

As a result of these concerns, on August 7, 2001, this Court ordered the United States to file with the Court a report explaining fully how the KLS device functions and describing the KLS technology and how it works vis-à-vis the computer modem, Internet communications, e-mail and all other uses of a computer. In light of the government's grave concern over the national security implications such a revelation might raise, the Court permitted the United States to submit any additional evidence which would provide particular and specific reasons how and why disclosure of the KLS would jeopardize both ongoing and future domestic criminal investigations and national security interests.

The United States responded by filing a request for modification of this Court's August 7, 2001, Letter Opinion and Order so as to comply with the procedures set forth in the Classified Information Procedures Act, Title 18, United States Code, Appendix III, § 1 *et seq.* ("CIPA"). This request, of course, presented a new wrinkle into what had been an already intriguing case. Defendant Scarfo objected to the government's request, alleging that the United States did not make a sufficient showing that the information concerning the KLS had been properly classified.

In response to Scarfo's objection, the United States submitted the affidavit of Neil J. Gallagher, Assistant Director, Federal Bureau of Investigation, dated September 6, 2001. In his affidavit, Mr. Gallagher stated that the characteristics and/or functional components of the KLS were previously classified and marked "SECRET" at or around November 1997.

The Court heard oral argument on September 7, 2001, to explore whether the government may invoke CIPA and, specifically, whether the government had classified the KLS. Although the defense conceded that the KLS was classified for purposes of CIPA,[1] the Court reserved on that question and ordered the government to provide written submissions to the Court. The government then filed an *ex parte, in camera* motion for the Court's inspection of the classified material.

On September 26, 2001, the Court held an *in camera, ex parte* hearing with several high-ranking officials from the United States Attorney General's office and the F.B.I. Because of the sensitive nature of the material presented, all CIPA regulations were followed and only those persons with top-secret clearance were permitted to attend. Pursuant to CIPA's regulations, the United States presented the Court with detailed and top-secret, classified information regarding the KLS, including how it operates in connection with a modem. The government also demonstrated to the Court how the KLS affects national security.

After reviewing the classified material, I issued a Protective Order pursuant CIPA on October 2, 2001, wherein I found that ***576** the government could properly invoke CIPA and that the government made a sufficient showing to warrant the issuance of an order protecting against disclosure of the classified information. The October 2, 2001, Protective Order also directed that the government's proposed unclassified summary of information relating to the KLS under Section 4 of CIPA would be sufficient to allow the defense to effectively argue the motion to suppress. Accordingly, the Protective Order permitted the government to provide Scarfo with the unclassified summary statement in lieu of the classified information regarding the KLS. Pursuant to Section 6(d) of CIPA, the Court also sealed the transcript of the September 26th *ex parte, in camera* hearing and the government's supporting Affidavits. The government filed with the Court and served on Scarfo the unclassified summary on October 5, 2001, in the form of an October 4, 2001, Affidavit of Randall S. Murch, Supervisory Special Agent of the Federal Bureau of Investigation, Laboratory Division (the "Murch Affidavit").

Having the benefit of the September 26th *ex parte, in camera* hearing and the many supplemental submissions of the parties, the Defendants' motion for discovery and suppression is now ripe for resolution.

DISCUSSION

Defendants Scarfo and Paolercio advance several arguments in moving to suppress certain evidence seized by the FBI. The Defendants first contend that the KLS constituted an unlawful general warrant in violation of the Fourth Amendment to the Constitution. In addition, the Defendants, after reviewing the government's unclassified summary, i.e., the Murch Affidavit, argue that the Murch Affidavit is inadequate under CIPA and would conflict with the United States Supreme Court decision of *Jencks v. United States,* 353 U.S. 657, 77 S. Ct. 1007, 1 L. Ed. 2d 1103 (1957).

Lastly, Defendants urge the Court to suppress the evidence because the KLS effectively intercepted a wire communication in violation of Title III, 18 U.S.C. § 2510.

I. *General Warrant*

Scarfo argues that since the government had the ability to capture and record only those keystrokes relevant to the "passphrase" to the encrypted file, and because it received an unnecessary overcollection of data, the warrants were written and executed as general warrants. This claim is without merit.

Typically, the proponent of a motion to suppress bears the burden of establishing that his Fourth Amendment rights were violated. *See United States v. Acosta,* 965 F.2d 1248, 1257 n. 9 (3d Cir. 1992) (citing *Rakas v. Illinois,* 439 U.S. 128, 130 n. 1, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1979)). The standard of proof in this regard is a preponderance of the evidence. *See United States v. Matlock,* 415 U.S. 164, 178 n. 14, 94 S. Ct. 988, 39 L. Ed. 2d 242 (1974) ("[T]he controlling burden of proof at suppression hearings should impose no greater burden than proof by a preponderance of the evidence.").

It is settled that at a hearing on a motion to suppress, "the credibility of the witnesses and the weight to be given the evidence, together with the inferences, deductions and conclusions to be drawn from the evidence, are all matters to be determined by the trial judge." *United States v. McKneely,* 6 F.3d 1447, 1452-53 (10th Cir.1993). *See also United States v. Matthews,* 32 F.3d 294, 298 (7th Cir.1994); *United States v. Cardona-Rivera,* 904 F.2d 1149, 1152 (7th Cir.1990); *Government of the Virgin Islands v. Gereau,* 502 ***577** F.2d 914, 921 (3d Cir.1974), *cert. denied,* 420 U.S. 909, 95 S. Ct. 829, 42 L. Ed. 2d 839 (1975).

The Fourth Amendment states that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Where a search warrant is obtained, the Fourth Amendment requires a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized. *See Torres v. McLaughlin,* 163 F.3d 169, 173 (3d Cir.1998), *cert. denied,* 528 U.S. 1079, 120 S. Ct. 797, 145 L. Ed. 2d 672 (2000). The particularity requirement exists so that law enforcement officers are constrained from undertaking a boundless and exploratory rummaging through one's personal property. *See United States v. Johnson,* 690 F.2d 60, 64 (3d Cir.1982) (citing *Coolidge v. New Hampshire,* 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971)), *cert. denied,* 459 U.S. 1214, 103 S. Ct. 1212, 75 L. Ed. 2d 450 (1983).

From a review of the two Court Orders authorizing the searches along with the accompanying Affidavits, it is clear that the Court Orders suffer from no constitutional infirmity with respect to particularity. Magistrate Judge Donald Haneke's May 8, 1999, Order permitting the search of Scarfo's computer clearly states that Judge Haneke found probable cause existed to believe that "Nicodemo S. Scarfo has committed and continues to commit offenses in violation of Title 18, U.S.C. §§ 371, 892-94, 1955 and § 1962." *See* Judge Haneke's May 8, 1999 Order, at ¶ 1. That Order further stated that there was "probable cause to believe that Nicodemo S. Scarfo's computer, located in the TARGET LOCATION, is being used to store business records of Scarfo's illegal gambling business and loansharking operation, and that the above mentioned records have been encrypted." *See* Judge Haneke's May 8, 1999 Order, at ¶ 3.

Because the encrypted file could not be accessed via traditional investigative means, Judge Haneke's Order permitted law enforcement officers to "install and leave behind software, firmware, and/or hardware equipment which will monitor the inputted data entered on Nicodemo S. Scarfo's computer in the TARGET LOCATION so that the F.B.I. can capture the password necessary to decrypt computer files by recording the key related information as they are entered." *See* Judge Haneke's May 8, 1999 Order, at pp. 4. The Order also allowed the F.B.I. to

> search for and seize business records in whatever form they are kept (e.g., written, mechanically or computer maintained and any necessary computer hardware, including computers, computer hard drives, floppy disks or other storage disks or tapes as necessary to access such information, as well as, seizing the mirror hard drive to preserve configuration files, public keys, private keys, and other information that may be of assistance in interpreting the password)including address and telephone books and electronic storage devices; ledgers and other accounting-type records; banking records and statements; travel records; correspondence; memoranda; notes; calendars; and diaries that contain information about the identities and whereabouts of conspirators, betting customers and victim debtors, and/or that otherwise reveal the origin, receipt, concealment or distribution of criminal proceeds relating to illegal gambling, loansharking and other racketeering offenses.

See Judge Haneke's May 8, 1999 Order, at pp. 4-5.

***578** On its face, the Order is very comprehensive and lists the items, including the evidence in the encrypted file, to be seized with more than sufficient specificity. *See Andresen v. Maryland,* 427 U.S. 463, 480-81, 96 S. Ct. 2737, 2748-49, 49 L. Ed. 2d 627 (1976) (defendant's general warrant claim rejected where search warrant contained, among other things, a lengthy list of specified and particular items to be seized). One would be hardpressed to draft a more specified or detailed search warrant than the May 8, 1999 Order.[2] Indeed, it could not be written with more particularity. It specifically identifies each piece of evidence the F.B.I. sought which would be linked to the particular crimes the F.B.I. had probable cause to believe were committed. Most importantly, Judge Haneke's Order clearly specifies the key piece of the puzzle the F.B.I. sought Scarfo's passphrase to the encrypted file.

That the KLS certainly recorded keystrokes typed into Scarfo's keyboard *other* than the searched-for passphrase is of no consequence. This does not, as Scarfo argues, convert the limited search for the passphrase into a general exploratory search. During many lawful searches, police officers may not know the exact nature of the incriminating evidence sought until they stumble upon it. Just like searches for incriminating documents in a closet or filing cabinet, it is true that during a search for a passphrase "some innocuous [items] will be at least cursorily perused in order to determine whether they are among those [items] to be seized." *United States v. Conley,* 4 F.3d 1200, 1208 (3d Cir.1993). *See also United States v. Carmany,* 901 F.2d 76 (7th Cir.1990) (upholding seizure of unregistered handgun found in filing cabinet while validly executing warrant to discover evidence relating to cocaine distribution charges) *United States v. Fawole,* 785 F.2d 1141, 1145 (4th Cir. 1986); *United States v. Santarelli,* 778 F.2d 609, 615-16 (11th Cir.1985) (search warrant entitled agents to search for documents, i.e., records of loansharking activity, etc., and agents were entitled to examine each document in bedroom or in filing cabinet to determine whether it constituted evidence they were entitled to seize under warrant); *United States v. Issacs,* 708 F.2d 1365, 1368-70 (9th Cir.), *cert. denied,* 464 U.S. 852, 104 S. Ct. 165, 78 L. Ed. 2d 150 (1983); *United States v. Christine,* 687 F.2d 749, 760 (3d Cir.1982).

Hence, "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision." *Conley,* 4 F.3d at 1208 (quoting *United States v. Christine,* 687 F.2d 749, 760 (3d Cir.1982)). Where proof of wrongdoing depends upon documents or computer passphrases whose precise nature cannot be known in advance, law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant. As the Supreme Court stated in *Andresen,* "the complexity of an illegal scheme may not be used as a shield to avoid detection when the [government] has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession." *Andresen,* 427 U.S. at 482, 96 S. Ct. at 2749 n. 10. Accordingly, Scarfo's claim that the warrants were written and executed as general warrants is rejected.

579 II. *Jencks Argument

Scarfo next contends that the use of the Murch Affidavit would pose a direct conflict with the Supreme Court's decision in *Jencks v. United States,* 353 U.S. 657, 77 S. Ct. 1007, 1 L. Ed. 2d 1103 (1957). For several reasons, this claim also lacks merit.[3]

The plainest answer to Scarfo's invocation of *Jencks* is that it simply does not apply in this context. The Jencks Act, which bears its name from the famous *Jencks* Supreme Court ruling, requires the government to disclose prior recorded statements of its witnesses, when related to the subject matter of their testimony, after each witness testifies on direct examination. *See* 18 U.S.C.A. § 3500(b); *United States v. Weaver,* 267 F.3d 231, 245 (3d Cir.2001). Its primary purpose is to allow the defense to utilize on cross-examination a government witness' prior testimony or statements to impeach the witness. *See Goldberg v. United States,* 425 U.S. 94, 107, 96 S. Ct. 1338, 1346, 47 L. Ed. 2d 603 (1976). Here, the discovery sought by Scarfo does not involve a government witness, but rather the KLS device. Hence, no Jencks conflict arises.[4]

As the Court will explain more fully below, Scarfo will not be "crippled" in his ability to defend himself in the prosecution of this case if his discovery request is denied. The Court has determined that, pursuant to Section 4 of CIPA, the unclassified summary in the form of the Murch Affidavit will provide Scarfo with all the information that is necessary to litigate this motion.

Defendant Scarfo is also mistaken in asserting that the government's obligation to produce and disclose information during the course of the criminal discovery process is absolute. Although typically the government owes an ongoing duty to disclose information to the defense, the Congress has, by statute, carved out exceptions. CIPA is one such example.

III. *CIPA*

In relation to his argument that the KLS unlawfully intercepted a wire communication, Scarfo disputes the government's insistence that the Murch Affidavit is sufficient for purposes of litigating the suppression motion. Since the Court's October 2nd Protective Order deemed the Murch Affidavit sufficient for purposes of adjudicating this motion, Scarfo in essence asks the Court to reconsider that ruling.

Congress enacted CIPA on October 15, 1980, to address the issues which accompany criminal prosecutions involving national security secrets. CIPA establishes certain pretrial, trial and appellate procedures regarding the handling of classified information in criminal cases and protects against disclosure of sensitive, classified information. Section 1(a) of CIPA defines the term "classified information" as follows:

> any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph ***580** r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. § 2014(y)).

The term "national security" is defined in Section 1(b) of the Act as "the national defense and foreign relations of the United States."

Section 2 allows "any party [to] move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution." Section 6(a) sets forth the procedure for hearing a motion in a case involving classified information:

> Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection ... shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.

After hearing such a motion, Section 4 permits the court, upon a sufficient showing, to authorize the United States to substitute a summary of the information the defendant seeks for the classified documents. This section also authorizes the court to seal and preserve in the records of the court the entire text of the statement.

Section 6(c) also prescribes a similar procedure for the disclosure of classified information. Under Section 6(c), the government may seek an order permitting the substitution for the classified information of a summary statement of the specific classified information. Where the court finds that the summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information, the court shall allow the government to file the summary in lieu of complete disclosure of the classified information. Section 6(d) authorizes the court to seal the record of any *in camera* hearings held pursuant to CIPA.

Pursuant to CIPA, the United States requested a hearing in order to block the disclosure of supposedly classified information concerning the KLS technique. The Court held an *in camera, ex parte* hearing on September 26, 2001, to assess the classified nature of the KLS and the sufficiency of the unclassified summary proposed by the government. Prior to the September 26th *in camera, ex parte* hearing, and as expressed during the September 7th hearing, the Court was not satisfied that the KLS was properly classified as defined by CIPA. Nor was the Court at the time content with the United States' conclusory and generalized expressions of concern that revelation of the KLS would compromise the national security of the United States.

However, as a result of the September 26th *in camera, ex parte* hearing, the Court is now satisfied that the KLS was in fact classified as defined by CIPA. The Court also concludes that under Section 4 and 6(c) of CIPA the government met its burden in showing that the information sought by the Defendants constitutes classified information touching upon national security concerns as defined in CIPA. ***581** Moreover, it is the opinion of the Court that as a result of the September 26th hearing, the government presented to the Court's satisfaction proof that disclosure of the classified KLS information would cause identifiable damage to the national security of the United States. The Court is precluded from discussing this information in detail since it remains classified.

Further, upon comparing the specific classified information sought and the government's proposed unclassified summary, the Court finds that the United States met its burden in showing that the summary in the form of the Murch Affidavit would provide Scarfo with substantially the same ability to make his defense as would disclosure of the specific classified information regarding the KLS technique. The Murch Affidavit explains, to a reasonable and

sufficient degree of specificity without disclosing the highly sensitive and classified information, the operating features of the KLS. The Murch Affidavit is more than sufficient and has provided ample information for the Defendants to litigate this motion. Therefore, no further discovery with regard to the KLS technique is necessary.

IV. *Whether the KLS Intercepted Wire Communications*

The principal mystery surrounding this case was whether the KLS intercepted a wire communication in violation of the wiretap statute by recording keystrokes of e-mail or other communications made over a telephone or cable line while the modem operated. These are the only conceivable wire communications which might emanate from Scarfo's computer and potentially fall under the wiretap statute.

Upon a careful and thorough review of the classified information provided to the Court on September 26th and the Murch Affidavit, the Court finds that the KLS technique utilized in deciphering the passphrase to Scarfo's encrypted file did not intercept any wire communications and therefore did not violate the wiretap statute, Title III, 18 U.S.C. § 2510. I am satisfied the KLS did not operate during any period of time in which the computer's modem was activated.

Scarfo's computer contained an encryption program called PGP (Pretty Good Privacy), which is used to encrypt or scramble computer files so that decrypting or unscrambling the files requires use of the appropriate passphrase. According to the Murch Affidavit, in order to decrypt an encrypted file, the PGP software displays on the user's computer screen a "dialog box." *See* Murch Aff., ¶ 3. The user then must enter, via the keyboard, the "passphrase" into the dialog box. *See id.* When the proper passphrase is entered, PGP verifies that the passphrase is correct and, after several steps, leads to the decryption of the selected file. *See id.*

The KLS, which is the exclusive property of the F.B.I., was devised by F.B.I. engineers using previously developed techniques in order to obtain a target's key and key-related information. *See* Murch Aff., ¶ 4. As part of the investigation into Scarfo's computer, the F.B.I. "did not install and operate any component which would search for and record data entering or exiting the computer from the transmission pathway through the modem attached to the computer." Murch Aff., ¶ 5. Neither did the F.B.I. "install or operate any KLS component which would search for or record any fixed data stored within the computer." *See id.*

Recognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the F.B.I. configured the KLS to avoid intercepting electronic communications typed on the keyboard and simultaneously ***582** transmitted in real time via the communication ports. *See* Murch Aff., ¶ 6. To do this, the F.B.I. designed the component "so that each keystroke was evaluated individually." *See id.* As Mr. Murch explained:

> The default status of the keystroke component was set so that, on entry, a keystroke was normally *not* recorded. Upon entry or selection of a keyboard key by a user, the KLS checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

Murch Aff., ¶ 6.

Hence, when the modem was operating, the KLS did not record keystrokes. It was designed to prohibit the capture of keyboard keystrokes whenever the modem operated. *See* Murch Aff., ¶ 15. Since Scarfo's computer possessed no other means of communicating with another computer save for the modem, *see* Murch Aff., ¶ 6, the KLS did not intercept any wire communications.[5] Accordingly, the Defendants' motion to suppress evidence for violation of Title III is denied.

Lastly, because the Court has determined that the Murch Affidavit is sufficient to argue the suppression motion, Scarfo's request for the discovery items listed in Dr. Farber's Affidavit is denied. Scarfo also asks, in the alternative, for the Court to certify these issues for appeal to the Court of Appeals for the Third Circuit. Although Section 7 of CIPA provides for interlocutory appeals, it appears to only permit the United States to appeal in the event of an adverse ruling. And the general statute permitting interlocutory appeals, 28 U.S.C. 1292(b), deals exclusively with civil actions. Nor would the collateral order doctrine permit an interlocutory appeal here, since this issue is readily reviewable on appeal in the event of a final judgment. *See Flanagan v. United States,* 465 U.S. 259, 265, 104 S. Ct. 1051, 1055, 79 L. Ed. 2d 288 (1984).

In fact, interlocutory appeals during a criminal prosecution are typically limited to three narrow classes of cases: denial of a motion to dismiss based on the Double Jeopardy Clause, requiring the posting of excessive bail, and violations of the Speech or Debate Clause. *See United States v. Miller,* 14 F.3d 761, 764-65 (2d Cir.1994) (citing

cases). *See also United States v. Helmsley,* 864 F.2d 266, 268-70 (2d Cir. 1988) (dismissing appeal as not falling within any of the three types of criminal cases meeting the collateral order exception), *cert. denied,* 490 U.S. 1065, 109 S. Ct. 2063, 104 L. Ed. 2d 628 (1989). Consequently, there appears to be no mechanism by which this Court could certify a question to the Third Circuit. And even if the Court could certify this issue to the Third Circuit it would not be inclined to do so.

Let there be no doubt that the courts are indeed the last bastions of freedom in our society and serve to protect the individual liberty rights embedded in our Constitution. The right to be free of unreasonable searches and seizures, the right to privacy and the right to a fair trial are among the most cherished of these rights. The Court's ruling herein is in consonance with these treasured ideals. The Congress has spoken through CIPA and determined that certain classified pieces of ***583** information implicate national security concerns to such a degree that disclosure of such information would seriously compromise United States' national security interests. In this way, CIPA strikes a balance between national security interests and a criminal defendant's right to discovery by allowing for a summary which meets the defendant's discovery needs.

In this day and age, it appears that on a daily basis we are overwhelmed with new and exciting, technologically-advanced gadgetry. Indeed, the amazing capabilities bestowed upon us by science are at times mind-boggling. As a result, we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. This includes the ability to find new ways to commit old crimes, as well as new crimes beyond the comprehension of courts. *See* Eric J. Sinrod, William P. Reilly, *Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws,* 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 177, 178-79 (2000). As a result of this surge in so-called "cyber crime," law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.

Accordingly, the Defendants' motion for discovery is granted in part and denied in part; specifically, the Defendants' request for the complete disclosure of the classified information is denied, but the motion is granted insofar as they are entitled to receive the unclassified summary in the form of the Murch Affidavit. The Defendants' motion to suppress evidence is denied.[6]

CONCLUSION

For the foregoing reasons, the motion to suppress evidence by Defendants Scarfo and Paolercio be and hereby is DENIED. The motion for discovery by Defendants Scarfo and Paolercio be and hereby is GRANTED IN PART and DENIED IN PART. Specifically, the Defendants' request for complete disclosure of the classified information concerning the KLS is DENIED. The Defendants are entitled to discovery consisting of the summary in the form of the Murch Affidavit.

IT IS SO ORDERED.

NOTES

[1] The defense argued the KLS was not classified "properly." *See* Transcript of September 7, 2001, hearing at 6:19-20.

[2] The second Order to search Scarfo's premises issued by Judge Haneke, dated June 9, 1999, contains identical language as the May 8, 1999 Order, and merely served to extend the period of the search for another thirty days.

[3] The Court notes in passing that in a legal memorandum addressing the instant motion submitted to and received by the Court on August 1, 2001, Scarfo's counsel conceded that "*Jencks* remedies do not appear to be directly available...." *See* Supplemental Brief of Defendant Nicodemo S. Scarfo, at 15.

[4] Neither does a *Brady* conflict exist, since the October 2nd Protective Order expressly states that "none of the material sought to be protected constitutes material that is subject to disclosure under *Brady v. Maryland,* 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963)." *See* Protective Order dated October 2, 2001.

[5] In addition, since all of the PGP program's functions and operations originated from the computer's hard drive, all actions involving either encryption or decryption occurred only within Scarfo's computer, and not on some other networked computer connected via modem. *See* Murch Aff., ¶ 8.

[6] Two other minor arguments by Scarfo also fail. The fact that a Bill called the Cyberspace Electronic Security Act ("CESA") of 1999 died in Congress before being acted upon has no relevance here. Moreover, the fact that the government may have revealed its "sniffer log program" in an unrelated Seattle case is of no moment. First, it

appears that the copy of the affidavit used in that case references a software program called "winwhatwhere," which can be purchased by anyone in retail stores or at "winwhatwhere's" website. *See* www.winwhatwhere.com. Secondly, that affidavit does not reveal any information at all about how the program works, but rather only states that the program was used by F.B.I. agents.